IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: David John Craft	§	
	§	
Serial Number: 10/601,374	§	
	§	Group Art Unit: 2136
Filed: June 23, 2003	§	
	§	
For: SECURITY ARCHITECTURE FOR SYSTEM ON CHIP	§	Examiner: Carlton Johnson
	§	
	§	
	§	

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, Virginia 22313-1450

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 37 C.F.R. § 1.8, I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office at www.uspto.gov

on: December 28, 2007

/Bradley D. Ellis/
Bradley D. Ellis

APPLICANT'S APPEAL BRIEF

Applicant-inventor ("Applicant") and assignee International Business Machines Corporation respectfully submit the present brief in support of the patentability of the claims of the above-referenced application.

I. REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation, of Armonk, New York, assignee of the interests in the invention from the named inventors.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 22-37 are pending. Of these, Claims 22 and 31 are independent Claims. Claims 1-21 have been canceled. Applicants appeal the Examiner's rejections of Claims 22-27 and 29-36 35 U.S.C. §102(e) and Claims 28 and 37 under 35 U.S.C. §103(a).

IV. STATUS OF AMENDMENTS

The Claims stand as amended in the Response to an Office Action dated March 13, 2007.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Modern microprocessors, particularly networked processors, are increasingly equipped with or adapted for security mechanisms to provide authentication and encryption functions to be performed in the constituent networked processors. *See* Application, Page 1, Lines 9-15. One conventional method provides a hardware mechanism to ensure that the initial operating system image has not been tampered with. *See* Application, Page 2, Lines 5-7. This approach, however, depends on the Operating System (OSs) to maintain system integrity once the system has been started. *See* Application, Page 2, Lines 7-9. Therefore, this approach suffers from the disadvantage that has a drawback in that OSs are often very insecure. *See* Application, Page 2, Lines 9-14.

Another conventional system provides a separate security chip in the computer system, capable of providing the authentication, encryption, and key management functions, such as

those specified by the trusted computing alliance (TCA™). *See* Application, Page 2, Lines 15-20. A separate chip has the advantage that its interface protocols can be limited to security functions, which can make it very difficult to mount a software attack on such a chip. *See* Application, Page 2, Lines 20-23. However, because the security chip is separate from the microprocessor, it is relatively easy to monitor the interfaces and circumvent the protocols, and therefore does not provide good protection for implementing a secure boot function because the authenticated operating system image can relatively easily be replaced. *See* Application, Page 2, Lines 23-29.

Another conventional system provides an integrated security unit connected to the processor input/output (I/O) or the memory interface. *See* Application, Page 2, Lines 30-33. Because these integrated security devices provide the authentication and/or encryption functions on the processor chip, this unit is not easily monitored, and therefore provides a higher degree of protection than a separate security chip. *See* Application, Page 3, Lines 1-6. However, this arrangement suffers from significant disadvantages in that the security unit can occupy a significant silicon area on the processor chip, which is typically implemented in significantly more expensive technology and that such a unit, if it is to be realized at a reasonable cost (area), can provide basic functionality only. *See* Application, Page 3, Lines 6-12.

The present invention, defined in Claims 22-37, solves these and other problems by providing a novel method and apparatus for secure processing, particularly authenticating code and/or data and providing a protected environment for execution. *See* Application, Page 19, Lines 4-6. The novel method and apparatus dynamically partitions and un-partitions a local store for the authentication of code or data. *See* Application, Page 19, Lines 6-8. The local store is partitioned into an isolated and non-isolated section and code or data is loaded into the isolated

section. *See* Application, Page 19, Lines 8-10. The code or data is authenticated in the isolated section of the local store and then executed. *See* Application, Page 19, Lines 10-12. After execution, the memory within the isolated region is erased and de-partitioned. *See* Application, Page 19, Lines 12-16.

The Claims embody the invention as follows, as indicated in the Independent Claims shown below with illustrative citations to page and line numbers in the Original Application designated in curved braces ("{}"):

Claim 22: A secure processing system, comprising: {Page 5, Lines 14-17}

a main processor unit (MPU) coupled to a processor bus; {Page 5, Line 31}

an attached processor complex (APC) coupled to the processor bus and comprising: {Page 5, Lines 17-27}

a local store configured to store computer instructions and data; {Page 5, Lines 15-16}

an attached processor unit (APU) coupled to the local store; {Page 5, Lines 18-19}

wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; and {Page 6, Lines 1-15; 23-25}

wherein in response to a LOAD command received from the MPU, the APC is configured to transition from the non-isolated state to the isolated state, to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU, to transfer a set of computer instructions or data into the isolated section of the local store, and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key. {Page 7; Lines 3-20}

Claim 31: A method for carrying out secure processing, comprising:

providing a main processor unit (MPU), a processor bus, and an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor unit (APU) coupled to the local store; {Page 5, Lines 15-31}

configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required; {Page 7, Lines 3-7}

coupling the MPU to the processor bus; {Page 5, Line 31}

configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; {Page 6, Lines 1-9}

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state; {Page 5, Lines 15-17}

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU; {Page 6, Lines 16-26}

transferring a set of computer instructions or data into the isolated section of the local store; {Page 7, Lines 10-14}

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; and {Page 7, Lines 10-14}

coupling the APC to the processor bus. {Page 6, Lines 5-7}

VI. GROUNDS OF REJECTION TO BE REVIEWED

Whether Claims 22-27 and 29-36 are patentable over Ellison et al. (US 7,082,615).

Whether Claims 28 and 37 are patentable over Ellison in view of Worley Jr. et al. (US PGPUB 2002/0194389).

VII. ARGUMENT

A. Grouping of Claims

Claims 22 and 31 are independent. For purposes of this appeal, Applicant considers each of the independent Claims, and their respective dependent Claims, as separate groups. Thus, the groups of Claims are 22-30 and 31-37.

B. Summary of Pertinent Prosecution

Applicant filed the present application on June 23, 2003, with 21 claims.

The Examiner mailed the first Office Action on November 29, 2006 ("First Action"), rejecting Claims 1-4, 6-8, and 10- 21 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison et al. (US 7,082,615)("Ellison") in view of Worley, Jr. et al. (US PGPUB 2002/0194389)("Worley"). Similarly, the Examiner rejected Claims 5 and 9 based on the combination of Ellison and Worley in view of Dahan et al. (US PGPUB 2003/0140244).

Applicant responded to the First Action on March 13, 2007 ("First Response"), cancelling Claims 1-21 and adding new Claims 22-37.

The Examiner mailed the Final Action under appeal on June 1, 2007 ("Final Action"). In the Final Action, the Examiner rejected Claims 22-27 and 29-36 under 35 U.S.C. §102(e) as allegedly anticipated by Ellison. The Examiner also rejected Claims 28 and 37 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison in view of Worley. This appeal followed.

C. The Examiner's Rejections

To support the rejection under Section 102(e), the Examiner asserts in the Final Action, among other things, that Ellison teaches "wherein in response to a LOAD command received from the MPU (see Ellison col. 3, lines 43-45: load command initiated by processor), the APC is configured . . . to partition the local store into a general access section accessible by the MPU

and an isolated section accessible only by the APU, to transfer a set of computer instructions or data into the isolated section of the local store (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code and data to isolated region)." Final Action, Page 3. The Examiner also asserts that Ellison teaches "configuring the APC to respond to a received LOAD command by: . . . partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU; (see Ellison col. 4, lines 16-22: partition into isolated and non-isolated sections)." Final Action, Page 6. The Examiner's rejections under Section 103 rely on the rejections under Section 102. *See* Final Action, Pages 9-10.

D. The Examiner's Rejections Were Procedurally and Factually in Error

1. The Form and Content of the Examiner's Rejections under Section 102 Were Improper and Insufficient

a. Legal Requirements for an Anticipation Rejection

The applicable statute, 35 U.S.C. §102(e), provides, in pertinent part:

> A person shall be entitled to a patent unless –
> (e) the invention was described in - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

To anticipate a Claim under Section 102, the cited reference must teach each and every element of the Claim. *See* Manual of Patent Examining Procedure (MPEP) Section 2131. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Further, "The identical invention must be shown in as complete detail as is contained in the . . . claim."

Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Finally, the claimed elements must be arranged as recited by the claim, but "identity of terminology" is not required. *See In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

In some instances, more than one reference may be employed to support a Section 102 rejection:

> Normally, only one reference should be used in making a rejection under 35 U.S.C. 102. However, a 35 U.S.C. 102 rejection over multiple references has been held to be proper when the extra references are cited to:
>
> (A) Prove the primary reference contains an "enabled disclosure;"
>
> (B) Explain the meaning of a term used in the primary reference; or
>
> (C) Show that a characteristic not disclosed in the reference is inherent.

MPEP Section 2131.01. Applicants note, however, that in this case, the Examiner has employed only one reference under Section 102(e). Accordingly, each Section 102 reference in this case must show each and every element of the Claims.

b. The Examiner's Stated Grounds Were Insufficient

As described above, the Examiner rejects Claims 1-27 and 29-36 under 35 U.S.C. §102(e) as allegedly anticipated by Ellison. *See* Final Action, Page 8. Applicant respectfully submits that these rejections are in error and should be withdrawn.

More particularly, the Examiner's stated grounds were insufficient because, at a minimum, the cited reference does not teach each and every element of the Claims. Specifically, Ellison does not teach, disclose, or suggest "wherein in response to a LOAD command received from the MPU, the APC is configured . . . to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 22, or "configuring the APC to respond to a received LOAD command by: . . . partitioning the

local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 31.

First, the Examiner does not provide any support in the reference for the element in question, although the Examiner does provide pinpoint citations to surrounding elements. For example, as described above, the Examiner cites Ellison at col. 3, Lines 43-45 as showing "in response to a LOAD command received from the MPU;" cites Ellison at col. 4, Lines 16-22 as purportedly showing that the "APC is configured to transition from the non-isolated state to the isolated state" in response to the LOAD command, and cites Ellison at col. 3, Lines 21-25 and 45-47 as purportedly showing "transfer a set of computer instructions or data into the isolated section of the local store" in response to the LOAD command. *See* Final Action, Page 3, Paragraph (d). But the Examiner provides no support in Ellison for the element between the last two elements above, "to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU" in response to the LOAD command. *See* Final Action, Page 3, Paragraph (d).

Because the Examiner has failed to provide support for this element, and considering the fact that the Examiner provided specific citations to the surrounding elements, Applicant must assume that the Examiner intends the entire reference to show, somewhere, a system configured "to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU" in response to the LOAD command. But nowhere does Ellison even hint at that element. As such, the Examiner's purported prima facie case must fail.

The citations do, however, demonstrate why Ellison nowhere teaches the missing element. Specifically, the cited passages prove that Ellison actually teaches away from "to partition the local store into a general access section accessible by the MPU and an isolated section accessible

only by the APU" in response to the LOAD command. For example, Ellison states: "The isolated execution mode is initialized using a privileged instruction in the processor, combined with the processor nub loader 52." Ellison, col. 3, lines 43-45. Here, at least, Ellison operates in a "isolated execution mode" in response to a "privileged instruction in the processor."

But Ellison distinguishes between its "isolated execution mode" and its pre-partitioned "isolated area": in the "isolated execution mode," "The processor nub loader 52 verifies and loads a ring-0 nub software module (e.g., processor nub 18) into the isolated area." Ellison, col. 3, lines 45-47. That is, the Ellison "isolated area" is not established in response to invoking the "isolated execution mode," the Ellison "isolated area" already exists prior to the "isolated execution mode." More particularly, "The logical operating architecture 50 [of Ellison] has two modes of operation: normal execution mode and isolated execution mode." Ellison, col. 3, lines 4-6. The Ellison architecture contains "rings" that are perpetually partitioned into "normal execution" portion and an "isolated execution" portion, for example: "Ring-0 10 includes two portions: a normal execution Ring-0 11 and an isolated execution Ring-O 15." Ellison, col. 3, lines 9-10.

Thus, because Ellison's isolated execution portion is perpetual, Ellison affirmatively teaches away from an "isolated section accessible only by the APU" that is partitioned "in response to a LOAD command," as recited in the claims. For at least this reason, Ellison fails to teach each and every element of the Claims, and therefore cannot support a proper rejection under Section 102.

Put more plainly, the Examiner asserts that Ellison shows transferring a set of computer instructions or data into the isolated section of the local store in response to the LOAD command, but NOT dynamically creating that isolated section in response to the LOAD command, as

recited in the claims. *See* Final Action, Page 3 (*citing* Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code and data to isolated region)." Because of this fatal defect in the Examiner's purported prima facie showing, the rejections under Section 102(e) are insufficient and must be withdrawn.

2. The Form and Content of the Examiner's Rejections under Section 103 Were Improper and Insufficient

a. Legal Requirements for an Obviousness Rejection

The obligation of the examiner to produce reasoning and evidence in support of obviousness is clearly defined at M.P.E.P. §2142:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

M.P.E.P. §2143 sets out the three basic criteria that a patent examiner must satisfy to establish a *prima facie* case of obviousness:

> 1. some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings;
> 2. a reasonable expectation of success; and
> 3. the teaching or suggestion of all the claim limitations by the prior art reference (or references when combined).

It follows that in the absence of such a *prima facie* showing of obviousness by the Examiner (assuming there are no objections or other grounds for rejection), an applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443 (Fed. Cir. 1992). Thus, in order to support an obviousness rejection, the Examiner is obliged to produce evidence compelling a conclusion that each of the three aforementioned basic criteria has been met.

b. The Examiner's Stated Grounds Were Insufficient

As described above, the Examiner rejects Claims 28 and 37 under 35 U.S.C. §103(a) as allegedly unpatentable over Ellison in view of Worley, Jr. *See* Final Action, Page 8. Applicant respectfully submits that these rejections are in error and should be withdrawn.

More particularly, as described above, Ellison wholly fails to teach, disclose, or suggest, and in fact teaches away from "wherein in response to a LOAD command received from the MPU, the APC is configured . . . to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 22 (from which Claim 28 depends), or "configuring the APC to respond to a received LOAD command by: . . . partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU," as recited in Claim 31 (from which Claim 37 depends).

The Examiner offers no suggestion that he provides Worley, Jr. to supply the elements missing from Ellison. *See* Final Action, Pages 9-11. Accordingly, for at least the above reasons, Applicant respectfully submits that the Examiner's proposed combination based on Ellison and Worley, Jr. fails to teach or disclose all of the elements and limitations of Claims 22-38. As such, the Examiner's proposed combination fails to support a prima facie case for obviousness under Section 103. Accordingly, the Examiner's rejections under Section 103(a) are insufficient and must also be withdrawn.

Based on all of the foregoing, Applicant respectfully submits that the Examiner's stated grounds are insufficient to maintain the Final Rejection. Applicant therefore respectfully requests that the Final Rejections be withdrawn and that Claims 22-37 be allowed.

VIII. CLAIMS APPENDIX

See Attached.

IX. EVIDENCE APPENDIX

NONE.

X. RELATED PROCCEDINGS APPENDIX

NONE.

XI. CONCLUSION

For the foregoing reasons, it is respectfully submitted that the Final Rejections of Claims 22-27 and 29-36 under 35 U.S.C. §102(e) and of Claims 28 37 under 35 U.S.C. §103(a) are improper and should be reversed. Applicants respectfully request that the rejections of Claims 22-37 be withdrawn and that Claims 22-37 be allowed.

Respectfully submitted,

/Gregory W. Carr/
Gregory W. Carr
Reg. No. 31,093

Dated: December 28, 2007
CARR LLP
670 Founders Square
900 Jackson Street
Dallas, Texas 75202
Telephone: (214) 760-3030
Fax: (214) 760-3003

VIII – APPENDIX – CLAIMS ON APPEAL

22. A secure processing system, comprising:

a main processor unit (MPU) coupled to a processor bus;

an attached processor complex (APC) coupled to the processor bus and comprising:

a local store configured to store computer instructions and data;

an attached processor unit (APU) coupled to the local store;

wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; and

wherein in response to a LOAD command received from the MPU, the APC is configured to transition from the non-isolated state to the isolated state, to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU, to transfer a set of computer instructions or data into the isolated section of the local store, and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key.

23. The secure processing system as recited in claim 22, wherein secure processing is performed within the isolated section of the local store of the APC.

24. The secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is not accessible by the MPU.

25. The secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is unique to the secure processing system.

26. The secure processing system as recited in claim 22, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store.

27. The secure processing system as recited in claim 22, wherein when the APC is operating in the isolated state, the APC is configured to respond to an EXIT command received from the MPU by clearing the isolated section of the local store and eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store.

28. The secure processing system as recited in claim 22, wherein the APC is configured to use the other cryptographic key to authenticate or decrypt another set of computer instructions or data.

29. The secure processing system as recited in claim 22, wherein the APC further comprises a bus interface unit (BIU) coupled to the processor bus, and wherein local store and the APU are coupled to the BIU.

30. The secure processing system as recited in claim 29, wherein the BIU comprises a load/exit state machine (LSEM) configured to store the cryptographic master key.

31. A method for carrying out secure processing, comprising:

providing a main processor unit (MPU), a processor bus, and an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor unit (APU) coupled to the local store;

configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required;

coupling the MPU to the processor bus;

configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state;

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state;

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU;

transferring a set of computer instructions or data into the isolated section of the local store;

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; and

coupling the APC to the processor bus.

32. The method as recited in claim 31, wherein the secure processing is carried out within the isolated section of the local store of the APC.

33. The method as recited in claim 31, wherein the cryptographic master key stored in the APC is not accessible by the MPU.

34. The method as recited in claim 31, wherein the coupling of the MPU and the APC to the processor bus forms a processing system, and wherein cryptographic master key stored in the APC is unique to the processing system.

35. The method as recited in claim 31, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store.

36. The method as recited in claim 31, further comprising:

configuring the APC to respond to a received EXIT command when operating in the isolated state by:

clearing the isolated section of the local store; and

eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store.

37. The method as recited in claim 31, wherein the configuring the APC to respond to a received LOAD command comprises:

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state;

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU;

transferring a set of computer instructions or data into the isolated section of the local store;

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic; and

using the other cryptographic key to authenticate or decrypt another set of computer instructions or data.